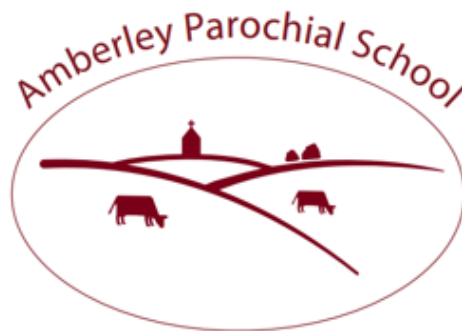


Online Safety Policy



**Providing the rich soil that enables
our children to develop deep roots and flourish.**

Chair of Governor: J Gegg and M Anderson

Approved by: FGB Committee

Approved on: Autumn Term One 2024

Review Date: Autumn Term One 2025

Other relevant policies: Safeguarding Policy, Special Educational Needs and Disabilities Policy, Computing and PSHCE Policies, Staff Code of Conduct Policy, Data Protection Policy,

This policy should be read in conjunction with KCSiE

Scope of the Policy

This policy applies to all members of the Amberley Parochial School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals¹ and groups within the school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
 - The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
 - The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
 - The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
-

- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead, which will be produced by ICT4 concepts, the IT service provider.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers (ICT4, SwGfL) in all aspects of filtering and monitoring.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The Governing body will ensure that appropriate filtering and monitoring systems are in place, they should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

The role of the Safeguarding Governor will include:

- Regular meetings with the DSL/online safety lead
- Regularly receiving (collated and anonymised) reports of online safety incidents
- Checking that provision outlined in the Online Safety Policy (e.g. Online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the [DfE Filtering and Monitoring Standards](#)
- Reporting to relevant Governors’ meetings
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safeguarding Lead (DSL)

The DSL will:

- Hold the lead responsibility for online safety, within their safeguarding role
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents, and filtering and monitoring logs, and ensuring that annual (at least) filtering and monitoring checks are carried out
- Attend relevant governing body meetings
- Report regularly to senior leadership team

- Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and IT providers (ICT4 / SWGfL) on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead:

At Amberley Parochial Primary School, the Online safety lead role will be part of the Designated Safeguarding Lead role. In this role, they will:

- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Have a leading role in establishing and reviewing the school online safety policies/documents
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- Liaise with (school/local authority/mat/external provider) technical staff, pastoral staff and support staff (as relevant)
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined in keeping children safe in education:
 - Content
 - Contact
 - Conduct
 - Commerce

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices, including the relevant sections of Keeping Children Safe in Education
- They understand that online safety is a core part of safeguarding
- They have read, understood and signed the Staff Acceptable Use Policy Agreement (AUP)
- They immediately report any suspected misuse or problem to the Head Teacher in their role as DSL/OSL for investigation/action, in line with the school safeguarding procedures
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and Acceptable Use policy Agreements
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider (ICT4):

It is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT provider is responsible for ensuring:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- The school technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets (as a minimum) the required online safety technical requirements as identified by the DfE 'Meeting Digital and Technology Standards in Schools & Colleges' and guidance from DGAT or other relevant body
- There is clear, safe, and managed control of user access to networks and devices
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Head Teacher in their role as DSL/OSL for investigation and action
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- Monitoring systems are implemented and regularly updated as agreed in school policies

Pupils:

- Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website
- Providing them with a copy of the learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- Publish information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- Reinforcing the online safety messages provided to learners in school.
- The safe and responsible use of their children's personal devices in the school (where this is allowed)

Community Users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy Statements

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils, students, and staff in their use of technology, and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within Online Safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- Allocates responsibilities for the delivery of the policy
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours

- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- Describes how the school will help prepare learners to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Is supplemented by a series of related acceptable use agreements
- Is made available to staff at induction and through normal communication channels (to be described)
- Is published on the school website.

Acceptable Use Policy

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable Use Agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated with staff, parents and pupils on an annual basis. Community users and guests will be asked to sign an agreement before being given access to the schools systems.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	<p>Any illegal activity for example:</p> <ul style="list-style-type: none"> • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering <p>If applicable, the school will refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges</p>					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) Gaining unauthorised access to school networks, data and files, through the use of computers/devices Creating or propagating computer viruses or other harmful files Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) Disable/Impair/Disrupt network functionality through the use of computers/devices Using penetration testing equipment (without relevant permission) 					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

When using communication technologies, the school considers the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) Must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community

- Users should immediately report to the Head Teacher/DSL – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

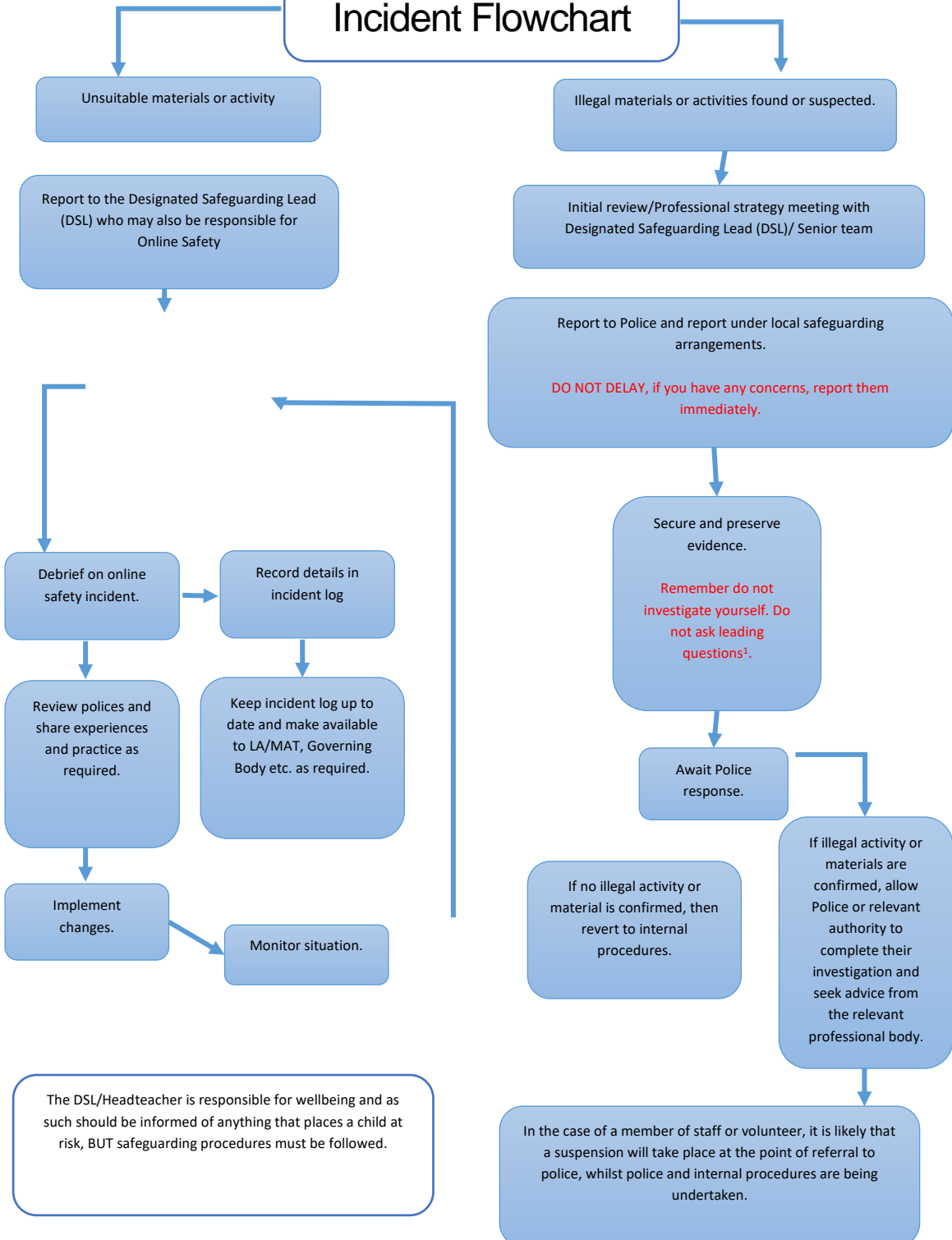
- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The designated safeguarding lead/online safety lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm ([see flowchart and user actions chart in the appendix](#)), the incident must be escalated through the agreed school safeguarding procedures. this may include
 - Non-consensual images
 - Self-generated images
 - Terrorism/extremism
 - Hate crime/ abuse
 - Fraud and extortion
 - Harassment/stalking
 - Child sexual abuse material (csam)
 - Child sexual exploitation grooming
 - Extreme pornography
 - Sale of illegal materials/substances
 - Cyber or hacking [offences under the computer misuse act](#)
 - Copyright theft or piracy
- Any concern about staff misuse will be reported to the headteacher, unless the concern involves the headteacher, in which case the complaint is referred to the chair of governors and DGAT.
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
 - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store

screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form

- Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by dgat
 - Police involvement and/or action
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- Incidents should be logged using the reporting template below
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. Local authority; police; [professionals online safety helpline](#); [reporting harmful content](#); [CEOP](#).
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - The governing body for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - Staff, through regular briefings
 - Learners, through assemblies/lessons
 - Parents/carers, through newsletters, school social media, website
 - Governors, through regular safeguarding updates
 - Local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Online Safety Incident Flowchart



Education –Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework (Using [Education for a Connected Work Framework by UKCIS/DCMS](#) and the [SWGfL Project Evolve](#)) and regularly taught in a variety of contexts, ensuring relevant and up to date objectives
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- The incorporation/ use of relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#)
- Accessibility to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- The active addressing of vulnerability as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- The development of an understanding of the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- Staff will act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Education – Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- The training will be an integral part of the school's annual safeguarding and data protection training for all staff.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It will include explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- The Designated Safeguarding Lead/ Online Safety Lead will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / DGAT / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days
- The DSL/OSL will provide advice/guidance/training to individuals as required.

Education – Governors

Governors take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by DGAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Education - Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, blog posts,
- Parents' / Carers' evenings / sessions

- The learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons
- High profile events / campaigns e.g. Safer Internet Day
- Reference to ~~the~~ relevant web sites / publications e.g. swgfl.org.uk
www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers
www.nationalonlinesafety.com ~~(see appendix for further links / resources)~~

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision when requested.

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider (ICT4/ SWGfL) and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider (ICT4).

- Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using [SWGfL Test Filtering](#)

Filtering

- The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the dfe [filtering standards for schools and colleges](#) and the guidance provided in the uk safer internet centre [appropriate filtering](#).
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the internet watch foundation url list and the police assessed list of unlawful terrorist content, produced on behalf of the home office. Content lists are regularly updated
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes
- Filtering logs are regularly reviewed and alert the designated safeguarding lead to breaches of the filtering policy, which are then acted upon.
- Younger learners will use child friendly/age-appropriate search engines e.g. Swgfl swiggle
- The school has a Staff Conduct policy and where personal mobile devices have internet access through the school network, content is filtered/managed in ways that are consistent with school policy and practice.
- Access to content through non-browser services (e.g. Apps and other mobile technologies) is filtered/ managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- Physical monitoring (adult supervision in the classroom)
- Internet use is logged, regularly monitored and reviewed
- Filtering logs are regularly analysed and breaches are reported to senior leaders
- Pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

- Use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- Responsibility for technical security resides with SLT who may delegate activities to identified roles.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT
- Password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- The security of their username and password and must not allow other users to access the systems using their log on details.
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- The administrator passwords for school systems are kept in a secure place, e.g. With ICT4
- There is a risk-based approach to the allocation of learner usernames and passwords.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- ICT4 Concepts are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- Staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- Removable media is not permitted unless approved by the SLT/IT service provider
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- Mobile device security and management procedures are in place
- Guest users are provided with appropriate access to school systems based on an identified risk profile and are expected to sign the relevant AUA before being given access.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The mobile technologies element of this policy is consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy Agreements, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users		Student owned	Staff owned (must be authorised)	Visitor owned
Allowed in school	Yes	Yes		No	Yes	Yes
<u>Access to school services (password controlled) Full network access</u>	Yes	<u>No/Yes</u>		No	Yes	No
<u>Filtered access to wifi</u>	<u>Yes</u>	<u>Yes</u>		<u>No</u>	<u>Yes</u>	<u>Yes</u>
<u>Unfiltered access to wifi</u>	<u>Yes</u>	<u>No</u>		<u>No</u>	<u>Yes</u>	<u>Yes (on request)</u>

School owned/provided devices:

- All school devices are managed through the use of Mobile Device Management software
- There is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- Personal use (e.g. Online banking, shopping, images etc.) Is clearly defined and expectations are well-communicated through the AUA
- The use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- Liability for damage aligns with current school policy for the replacement of equipment.
- Education is in place to support responsible use.

Personal devices:

- There is a clear policy (Staff Code of Conduct) covering the use of personal mobile devices on school premises for all users

- Where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- Where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.
- Use of personal devices for school business is defined in the acceptable use policy
- Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- The expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- Liability for loss/damage or malfunction of personal devices is clearly defined
- There is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- Education about the safe and responsible use of mobile devices is included in the school online safety education programmes

Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- Ensuring that personal information is not published.
- Education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Risk assessment, including legal risk.
- Guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- A process for approval by senior leaders
- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to personal social media sites during school hours

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others via DGAT policy and guidance.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- In accordance with [guidance from the Information Commissioner's Office](#), parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- Care should be taken when sharing digital/video images that learners are appropriately dressed
- Learners must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with online safety policy
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- [Permission](#) from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes
- Images will be securely stored in line with the school policy

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters

The school website is hosted by Wix.com. The school ensures that online safety policy has been

followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The School:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so.
- has paid the appropriate fee to the Information Commissioner's Office (ICO).
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed.
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this.
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice.

- has procedures in place to deal with the individual rights of the data subject,
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier.
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- understands how to share data lawfully and safely with other relevant data controllers .
- has clear and understood policies and routines for the deletion and disposal of data.
- reports any relevant breaches (via School Pro) to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software.
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school.
- only use encrypted data storage for personal data.
- will not transfer any school personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners, parents/carers, and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training.
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors.
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising.
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Acceptable Use Agreements:

Acceptable Use Agreements are now completed online using Microsoft forms.

[Click here](#) to access EYFS/ KS1 Acceptable Use Agreement

[Click here](#) to access KS2 Acceptable Use Agreement

[Click here](#) to access Staff/ Guest/ Volunteer Acceptable Use Agreement

[Click here](#) to access Community User Acceptable Use Agreement

Legislation:

Relevant legislation:

- [Education Act 1996](#)
- [Education and Inspections Act 2006](#)
- [Education Act 2011 Part 2 \(Discipline\)](#)
- [The School Behaviour \(Determination and Publicising of Measures in Academies\) Regulations 2012](#)
- [Health and Safety at Work etc. Act 1974](#)
- [Obscene Publications Act 1959](#)
- [Children Act 1989](#)
- [Human Rights Act 1998](#)
- [Computer Misuse Act 1990](#)